Lecture 1 - Computing Professional Ethics & Responsibilities

Introduction

- The term **ethics** refers to standards of moral conduct. For example, telling the truth is a matter of ethics. An unethical act is not always illegal, although it might be, but illegal acts would be viewed as unethical by most people. For example, purposely lying on a friend is unethical but usually not illegal, while perjuring oneself in a courtroom as a witness is both illegal and unethical. Whether or not criminal behavior is involved, ethics guide our behavior and play integral role in our lives.

- Much more ambiguous than the law, ethical beliefs can vary widely from one individual to another. Ethical beliefs may also vary based on one's religion, country, race, or culture. In addition, different ethical standards can apply to different areas of one's life. For example, **personal ethics** guide an individual's personal behavior; **business** or **professional ethics** guide an individual's or business's workspace behavior. Ethics with respect to the use of computers are referred to as **Computer Ethics**.

Computer Ethics

- Computer Ethics have taken on more significance in recent years because the proliferation of computers in the home and the workplace provides more opportunities for unethical acts than the past. The Internet also makes it easy to distribute information that some would view as unethical.
- or forward the most recent e-mail warning about a new computer virus to everyone in your address book.

- Businesses also deal with a variety of ethical issues in the course of normal business activities – from determining how many computers on which a particular software program should be installed, to identify how customer and employee information should be used, to deciding business practices. Business Ethics are the standards of conduct that guide a business's policies, decisions, and actions.

Business Ethics

- Businesses also deal with a variety of ethical issues during normal business activities – from determining how many computers on which a particular software program should be installed, to identify how customer and employee information should be used, to deciding business practices. Business Ethics are the standards of conduct that guide a business's policies, decisions, and actions.

Ethical Use of Copyrighted Material

- Both businesses and individuals should be very careful when copying, sharing, or otherwise using copyrighted material to ensure that the material is used in both a legal and an ethical manner.

- Common types of copyrighted material encountered on a regular basis include software, books, Web-based articles, music, and movies.

Books and Web-based Articles

- ▪ Print-based books, e-books, Web-based articles, and other types of literary material are all protected by copyright law. Consequently, they cannot be reproduced, presented as one's original material, or otherwise used in an unauthorized manner.

- Students, researchers, authors, and other writers need to be especially careful when using literary material as a resource for papers, articles, books, and so forth, to ensure the material is properly credited to the original author.

- To present someone else's work as your own is plagiarism, which is both a violation of copyright law and an unethical act. It can also get you fired.

- With the increased availability of online articles and fee-based online term paper services, some students might be tempted to create their papers by copying and pasting excerpts of online content into their documents. But these students should realize that this is plagiarism, and instructors can usually tell when a paper is created in this manner. There are also online sources instructors can use to test the originality of student papers. Many colleges and universities have strict consequences for plagiarism, such as automatically failing the assignment or course, or being expelled from the institution.

Plagiarism	Not Plagiarism
A student copying or retyping a few sentences or a few paragraphs written by another author to include in his term paper without crediting the original author.	A student copying or retyping a few sentences or a few paragraphs written by another author to include in his term paper, either indenting the quotation or placing it inside quotation marks, and crediting the original author with a citation in the text or with a footnote or endnote.

A newspaper reporter changing a few words in a sentence or paragraph written by another author and including the revised text in an article without crediting the original author.	A newspaper reporter changing a few words in a sentence or paragraph written by another author without changing the meaning of the text, including the revised text in an article, and crediting the original author with a proper citation.
A student copying and pasting information from various online documents to create her research paper without crediting the original author.	A student copying and pasting information from various online documents and using those quotes in her research paper either indenting or enclosed in quotation marks with the proper citation for each author.
A teacher sharing a poem with a class, leading the class to believe the poem was his original work.	A teacher sharing a poem with a class clearly identifying the poet.

ACM Code of Ethics and Professional Conduct

Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. The ACM Code of Ethics and Professional Conduct ("the Code") expresses the conscience of the profession.

The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Additionally, the Code serves as a basis for remediation when violations occur. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

Section 1 outlines fundamental ethical principles that form the basis for the remainder of the Code.

Section 2 addresses additional, more specific considerations of professional responsibility.

Section 3 guides individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member, and principles involving compliance with the Code are given in section 4.

Section 4. Commitment to ethical conduct is required of every ACM member, ACM SIG member, ACM award recipient, and ACM SIG award recipient. Principles involving compliance with the Code are given in Section 4.

The Code is concerned with how fundamental ethical principles apply to a computing professional's conduct. The Code is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision-making. When thinking through a particular issue, a computing professional may find that multiple principles should be considered, and that different principles will have different relevance to the issue. Questions related to these kinds of issues can best be answered by thoughtful consideration of the fundamental ethical principles, understanding that the public good is the paramount consideration. The entire computing profession benefits when the ethical decision-making process is accountable to and transparent to all stakeholders. Open discussions about ethical issues promote this accountability and transparency.

1. GENERAL ETHICAL PRINCIPLES

A computing professional should...

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority.

Computing professionals should consider whether the results of their efforts will respect diversity, will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work that benefits the public good.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should promote environmental sustainability both locally and globally.

1.2 Avoid harm

In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may lead to harm. When that harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified. In either case, ensure that all harm is minimized.

To minimize the possibility of indirectly or unintentionally harming others, computing professionals should follow generally accepted best practices unless there is a compelling ethical reason to do otherwise. Additionally, the consequences of data aggregation and emergent properties of systems should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation.

1.3 Be honest and trustworthy

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying

data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

Computing professionals should be honest about their qualifications, and about any limitations in their competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to either real or perceived conflicts of interest or otherwise tend to undermine the independence of their judgment. Furthermore, commitments should be honored.

Computing professionals should not misrepresent an organization's policies or procedures and should not speak on behalf of an organization unless authorized to do so.

1.4 Be fair and take action not to discriminate

The values of equality, tolerance, respect for others, and justice govern this principle. Fairness requires that even careful decision processes provide some avenue for redress of grievances.

Computing professionals should foster fair participation of all people, including those of underrepresented groups. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, bullying, and other abuses of power and authority, is a form of discrimination that, amongst other harms, limits fair access to the virtual and physical spaces where such harassment takes place.

The use of information and technology may cause new, or enhance existing, inequities. Technologies and practices should be as inclusive and accessible as possible and computing professionals should take action to avoid creating systems or technologies that disenfranchise or oppress people. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts

Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work. Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary for the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and work put into the public domain. Computing professionals should not claim private ownership of work that they or others have shared as public resources.

1.6 Respect privacy

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can

compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.

1.7 Honor confidentiality

Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities. A computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2. PROFESSIONAL RESPONSIBILITIES

A computing professional should...

2.1 Strive to achieve high quality in both the processes and products of professional work

Computing professionals should insist on and support high quality work from themselves and from colleagues. The dignity of employers, employees, colleagues, clients, users, and anyone else affected either directly or indirectly by the work should be respected throughout the process. Computing professionals should respect the right of those involved to transparent communication about the project. Professionals should be cognizant of any serious negative consequences affecting any stakeholder that may result from poor quality work and should resist inducements to neglect this responsibility.

2.2 Maintain high standards of professional competence, conduct, and ethical practice

High quality computing depends on individuals and teams who take personal and group responsibility for acquiring and maintaining professional

competence. Professional competence starts with technical knowledge and with awareness of the social context in which their work may be deployed. Professional competence also requires skill in communication, in reflective analysis, and in recognizing and navigating ethical challenges. Upgrading skills should be an ongoing process and might include independent study, attending conferences or seminars, and other informal or formal education. Professional organizations and employers should encourage and facilitate these activities.

2.3 Know and respect existing rules pertaining to professional work

"Rules" here include local, regional, national, and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs. Computing professionals must abide by these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. A rule may be unethical when it has an inadequate moral basis or causes recognizable harm. A computing professional should consider challenging the rule through existing channels before violating the rule. A computing professional who decides to violate a rule because it is unethical, or for any other reason, must consider potential consequences and accept responsibility for that action.

2.4 Accept and provide appropriate professional review

High quality professional work in computing depends on professional review at all stages. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of others' work.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks

Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations and testimony to employers, employees, clients, users, and the public. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Extraordinary care should be taken to identify and mitigate potential risks in machine learning systems. A system for which future risks cannot be reliably

predicted requires frequent reassessment of risk as the system evolves in use, or it should not be deployed. Any issues that might result in major risk must be reported to appropriate parties.

2.6 Perform work only in areas of competence

A computing professional is responsible for evaluating potential work assignments. This includes evaluating the work's feasibility and advisability, and making a judgment about whether the work assignment is within the professional's areas of competence. If at any time before or during the work assignment the professional identifies a lack of a necessary expertise, they must disclose this to the employer or client. The client or employer may decide to pursue the assignment with the professional after additional time to acquire the necessary competencies, to pursue the assignment with someone else who has the required expertise, or to forgo the assignment. A computing professional's ethical judgment should be the final guide in deciding whether to work on the assignment.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences

As appropriate to the context and one's abilities, computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. These communications with the public should be clear, respectful, and welcoming. Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing.

2.8 Access computing and communication resources only when authorized or when compelled by the public good

Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code. Consequently, computing professionals should not access another's computer system, software, or data without a reasonable belief that such an action would be authorized or a compelling belief that it is consistent with the

public good. A system being publicly accessible is not sufficient grounds on its own to imply authorization. Under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others.

2.9 Design and implement systems that are robustly and usably secure

Breaches of computer security cause harm. Robust security should be a primary consideration when designing and implementing systems. Computing professionals should perform due diligence to ensure the system functions as intended, and take appropriate action to secure resources against accidental and intentional misuse, modification, and denial of service. As threats can arise and change after a system is deployed, computing professionals should integrate mitigation techniques and policies, such as monitoring, patching, and vulnerability reporting. Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.

To ensure the system achieves its intended purpose, security features should be designed to be as intuitive and easy to use as possible. Computing professionals should discourage security precautions that are too confusing, are situationally inappropriate, or otherwise inhibit legitimate use.

In cases where misuse or harm are predictable or unavoidable, the best option may be to not implement the system.

3. PROFESSIONAL LEADERSHIP PRINCIPLES

Leadership may either be a formal designation or arise informally from influence over others. In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. While these principles apply to all computing professionals, leaders bear a heightened responsibility to uphold and promote them, both within and through their organizations.

A computing professional, especially one acting as a leader, should...

3.1 Ensure that the public good is the central concern during all professional computing work

People—including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing. The public good should always be an explicit consideration when evaluating tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group

Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities. Organizations—through procedures and attitudes oriented toward quality, transparency, and the welfare of society—reduce harm to the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation of computing professionals in meeting relevant social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to enhance the quality of working life

Leaders should ensure that they enhance, not degrade, the quality of working life. Leaders should consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be used in the workplace.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code

Leaders should pursue clearly defined organizational policies that are consistent with the Code and effectively communicate them to relevant stakeholders. In addition, leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated.

Designing or implementing processes that deliberately or negligently violate, or tend to enable the violation of, the Code's principles is ethically unacceptable.

3.5 Create opportunities for members of the organization or group to grow as professionals

Educational opportunities are essential for all organization and group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties. These opportunities should include experiences that familiarize computing professionals with the consequences and limitations of particular types of systems. Computing professionals should be fully aware of the dangers of oversimplified approaches, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and their contexts, and other issues related to the complexity of their profession—and thus be confident in taking on responsibilities for the work that they do.

3.6 Use care when modifying or retiring systems

Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work. Leaders should take care when changing or discontinuing support for system features on which people still depend. Leaders should thoroughly investigate viable alternatives to removing support for a legacy system. If these alternatives are unacceptably risky or impractical, the developer should assist stakeholders' graceful migration from the system to an alternative. Users should be notified of the risks of continued use of the unsupported system long before support ends. Computing professionals should assist system users in monitoring the operational viability of their computing systems, and help them understand that timely replacement of inappropriate or outdated features or entire systems may be needed.

3.7 Recognize and take special care of systems that become integrated into the infrastructure of society

Even the simplest computer systems have the potential to impact all aspects of society when integrated with everyday activities such as commerce, travel, government, healthcare, and education. When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded. That stewardship also requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, the ethical responsibilities of the organization or group are likely to change as well. Continual monitoring of how society is using a system will allow the organization or group to remain consistent with their ethical obligations outlined in the Code. When appropriate standards of care do not exist, computing professionals have a duty to ensure they are developed.

4. COMPLIANCE WITH THE CODE

A computing professional should...

4.1 Uphold, promote, and respect the principles of the Code

The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles of the Code and contribute to improving them. Computing professionals who recognize breaches of the Code should take actions to resolve the ethical issues they recognize, including, when reasonable, expressing their concern to the person or persons thought to be violating the Code.

4.2 Treat violations of the Code as inconsistent with membership in the ACM

Each ACM member should encourage and support adherence by all computing professionals regardless of ACM membership. ACM members who recognize a breach of the Code should consider reporting the violation to the ACM, which may result in remedial action as specified in the ACM's Code of Ethics and Professional Conduct Enforcement Policy.

Lecture 2 - Software Piracy & Digital Counterfeiting

Software Piracy

- Instead of stealing an existing computer program, object, or other valuable that belongs to someone else, software piracy and digital counterfeiting involve creating duplicates of these items, and then selling them or using them as authentic items.

- Software Piracy, the unauthorized copying of a computer program, is illegal in most of the countries, including Egypt. Because of the ease with which computers can create exact copies of software program, software piracy is a widespread problem.

- According to a recent report from the Business Software Alliance (BSA) – an organization formed by several of the world's leading software developers that has antipiracy programs in 75 counties worldwide – approximately 60% of all business application software globally (and about 40% of all business application software in the United States) is installed illegally. In more than half the countries studied, the software piracy rate exceeded 70%; in 24 countries, it was over 80% the report estimates that the monetary loss due to software piracy during 2020 was approximately $300 billion worldwide, and research firm IDC predicts that nearly $500 billion worth of software will be pirated in the next five years.

- Software Piracy can take many forms, including individuals making illegal copies of programs to give to friends, businesses installing software on more computers than permitted in the program's end-user license agreement, PC sellers installing unlicensed copies of software on PCs sold to consumers, and large-scale operations in which the software and its packaging are illegally duplicated and then sold as supposedly legitimate products.

- Pirated software – as well as pirated music CDs and movie DVDs – are commonly offered for sale at online auctions. They can also be downloaded from some Web sites and pear-to-pear file sharing services.

- Creating and distributing pirated copies of any type of intellectual Property (such as software, music, and movies) is illegal.

Digital Counterfeiting

- The availability of high-quality, full-color imaging products (such as scanners, color printers, and color copiers) has made digital counterfeiting – creating counterfeit copies of items, typically currency and other printed resources, using computers and other types of digital equipment – more viable and prevalent. According to the U.S. Secret Service, many of today's counterfeiters have moved from the traditional offset printing to digital counterfeiting. The U.S. Secret Service estimates that about 60% of all counterfeit money today is produced digitally – up from 0.025% in 2020.

- With digital counterfeiting, a document is scanned into a computer and then printed, or it is color-copied.

- In addition to counterfeiting currency, some criminals choose to create fake business checks or printed collectibles, such as football tickets, PCR and vaccine documents, even T-shirts.

- Other common digital counterfeiting activities include creating fake identification papers, such as corporate IDs, driver's licenses, passports, and visas.

- Counterfeiting is illegal in Egypt and is taken very seriously. For creating or knowingly circulating counterfeit currency, for instance, offenders can face up to 15 years in prison for each offense.

- Although most of the counterfeit currency is produced by serious criminals - such as organized crimes, gangs, and terrorist organizations – the Secret Service has seen a dramatic increase in counterfeiting among high school and college students. This is attributed primarily to the ease of creating counterfeit bills – although not necessarily high-quality counterfeit bills – with digital technology.

Protecting Against Software Piracy and Digital Counterfeiting

- Software piracy and digital counterfeiting affect more than big businesses and the government. Because software pirates cost software developers a great deal of money, these companies must charge higher prices and have less money available for research and development, which hurts law-abiding consumers.

- The following are some tools currently being used to fight software piracy and digital counterfeiting.

Education, Holograms, and Other Antipiracy Tools

- One noteworthy tool that the software industry is using in an attempt to prevent software piracy is **education**. By educating businesses and consumers about the legal use of software and the possible negative consequences associated with breaking antipiracy laws, the industry hopes to reduce the known use of illegal software significantly.

- Paired with this, the industry is continually working on strengthening antipiracy laws and adapting them to fit new technology, such as broadband Internet and rewritable DVDs. The industry is also working to find more convenient ways to deliver content quickly – such as over the Internet – to give consumers a legal option that is as fast as downloading a pirated version.

- To make it more difficult for criminals to create pirated copies of software, **holograms** – printed text or images that change their appearance when the item containing the hologram is titled or looked at from a different angle – are commonly used on CDs, DVDs, and stickers located on new PCs containing preinstalled software. Because holograms are difficult to duplicate, end users can feel confident that the software package they are buying or was installed on the PC they received is authentic if the hologram works correctly.

- Requiring a unique activation code – such as during a mandatory online product registration – before the software can be used or before certain key features of the program are unlocked is another antipiracy tool. Some software manufacturers have launched extensive campaigns – such as including information on their Web sites, in product information, and in advertisements – to inform consumers of how these precautions work and why they are needed.

- Other antipiracy techniques used by software companies include watching online auction sites and requesting the removal of suspicious items, and buying pirated copies of software via Web sites and then filing lawsuits against the sellers. The increase in prosecution of for illegally selling or sharing software, music, and movies may also help reduce some types of piracy and encourage individuals to obtain legal copies of these products.

- Digital imaging equipment (such as color copiers and scanners) is equipped with technologies that can be used to track currency and other counterfeit items created with these devices. For example, many color copiers print invisible codes on copied documents, making counterfeit money copied on those machines traceable. This type of technology is also thought to be incorporated into many scanners.

- Prevention measures against the counterfeiting of other types of documents – such as checks and identification cards – include using holograms, digital watermarks, and other difficult-to-reproduce content. A digital **watermark** is a subtle alteration that is not noticeable when the work is viewed or played, but that can be read using special software to authenticate the item.

- Finally, educating consumers about how the appearance of fake products differs from that of authentic products is a vital step in the ongoing battle against counterfeiting. Also, as countries with high levels of pirated software become more willing to fight piracy within their borders, the amount of global software piracy should drop as well.

Lecture 3 - Intellectual Property Rights

Introduction

- Like any fast-paced revolution, the computer revolution has impacted our society in more ways than could have been imagined when it first began.

- Computers often make daily tasks easier, but they also can make it easier to perform some types of illegal or unethical acts, can cause serious health and emotional problems, and can have a negative impact on the environment.

- In addition, although computer use is becoming almost mandatory in our society, many believe that access to computers is not equally available to all individuals.

INTELLECTUAL PROPERTY RIGHTS

- Intellectual Property Rights are the legal rights to which the creators of Intellectual property – original creative works – are entitled.

- Intellectual property rights indicate who has the right to the property; and other related restrictions.

- Examples of intellectual property include original music compositions; paintings, computer programs and graphics, and other works of art; poetry, books, and other types of written work; movies and video clips; architectural drawings; symbols, names, and designs used in conjunction with a business; and inventions.

- The three main types of intellectual property rights are:
  - Copyrights
  - Trademarks
  - Patents

Copyrights

- A copyright is a form of protection available for the creator of an original artistic or literary work, such as a book, movie, software program, musical composition, or painting.

- It gives the copyright holder the exclusive right to publish, reproduce, distribute, perform, or display the work.

- A major revision to U.S. copyright legislation was the 1976 Copyright Act. This act extended copyright protection to nonpublished works, so, immediately after creating a work in some type of material form (such as on paper, film, videotape, disk, CD, or DVD), the creator automatically owns the copyright of that work. Consequently, the creator is entitled to copyright protection of that work and has the right to make a statement, such as "Copyright © 2020 by Future University of Egypt, All rights reserved.", for example. It is wise to display this type of copyright statement on a published work to remind others that the work is protected by copyright law and that any use must comply with copyright law.

- Only the creator of a work (or his or her employer if the work is created as a work for hire – that is, within the scope of employment) can rightfully claim copyright. Copyrights can be registered with the Copyright Office. Although registration is not required for copyright protection, it does offer an advantage if the need to prove ownership of a copyright ever arises, such as during a copyright infringement lawsuit.

- Anyone wishing to use copyrighted material must first obtain permission from the copyright holder and pay any required fee. One exception is the legal concept of fair use, which permits limited duplication and use of a portion of the copyrighted material for certain purposes, such as criticism, commentary, news reporting, teaching, and research. For example, a teacher may legally read a copyrighted poem for discussion in a poetry class, and a news photographer may take a photograph of a newly installed sculpture to show on the evening news. Copyrights apply for both published and unpublished work and last until 70 years after the creator's death. Copyrights for work registered by an organization or as anonymous works last 95 years from the date of publication or 120 years from the date of creation, whichever is shorter.

- It is important to realize that purchasing a copyrighted item – such as a book, painting, or movie – does not change the copyright protection afforded to the creator of that item. Although you have purchased the right to use the item, you cannot legally duplicate it or portray it as your own creation. Some of the most widely publicized copyright-infringement issues today enter around individuals illegally distributing copyright-protected music and movies via the Internet.

- To protect their rights, some creators of digital content – such as art, music, photographs, and movies – incorporate Digital Watermarks containing copyright information into their works or use Digital Rights Management (DRM) Software to control the use of the work.

Trademarks

- A trademark is a word, phrase, symbol, or design (or combination of words, phrases, symbols, or designs) that identifies and distinguishes one product or service from another.

- Trademark rights prevent others from using a confusingly similar mark, but they do not prevent others from making or selling the same goods or services under a clearly different mark.

- Trademarks that are claimed but not registered with the U.S. Patent and Trademark Office can use the mark ™ ; registered trademarks can use the symbol ®.

- Trademarks words and phrases – such as Windows® 10 and BLOCKBUSTER® - are common; so are trademarked logos.

- Trademark law also protects domain names that match a company's trademark, such as Amazon.com and Lego.com.

- There have been several claims of online trademark infringement in recent years, particularly involving domain names that contain, or are similar to, a trademark. For instance, several celebrities – such as Madonna – have fought to be given the exclusive right to use what they consider their rightful domain names (Madonna.com, in this example). Other examples include Microsoft's complaint against another organization using the domain name microsoft.com and Radio Shack's objection to a private individual using shack.com for the Web site of his business called DesignShack.

Patents

- Unlike copyrights (which protect artistic and literary works) and trademarks (which protect a company's logo and brand names), a Patent protects inventions by granting exclusive rights of an invention to its inventor for a period of 20 years.

- A patented invention is typically a unique product, but it can also be a process or procedure that provides a new way of doing something or that offers a new technical solution to a problem.

- The number of patent applications – particularly for computer- or Internet-related products – has highly increased in recent years. Also growing the number of patents requested for business methods and models, such as Amazon.com's one-click purchase procedure, and others.

- When a product or business model is patented, no other organization can duplicate it without paying a royalty to the patent holder or risking prolonged patent litigation.

- Patents can be difficult, expensive, and time-consuming to obtain. However, patents can also be very lucrative. For instance, IBM – which has been the top patenting company for 12 consecutive years, was issued over 5,200 patents in 2020, and has over 90,000 active patents – earns an estimated $5 billion per year from its patents.